AFFIDAVIT OF SPECIAL AGENT KEVIN M. McCUSKER

I, Kevin M. McCusker, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent for the Federal Bureau of Investigation ("FBI") currently assigned to the Boston, Massachusetts Field Office. I have been so employed for over thirteen (13) years. Since August 2011, I have been assigned to the Boston Field Office economic crimes squad. Prior to this assignment, I investigated matters concerning National Security in the Minneapolis and Boston Field Offices. I hold a Bachelor's degree in Accounting and an inactive Certified Public Accountant license. As an FBI Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

2. I am submitting this affidavit in support a search warrant for 800 West Street, Unit 1417, Braintree, Massachusetts, which is further described in Attachment A (hereinafter, "the Target Location").

3. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses as well as my review of documents and bank records. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause to search the Target Location.

4. My affidavit submitted to the court in support of a criminal complaint on September 28, 2017, in case number 17-mj-6327-MPK charging YANNICK A. MINANG is incorporated herein by reference.

The Target Location

5. As further described in Attachment A, the Target Location is the apartment located at 800 West Street, Unit 1417, Braintree, Massachusetts within a group of apartments called the Ridge at Blue Hills. The Target Location, Unit 1417, is a two-bedroom apartment located on the top floor, at the corner of the building. The warrant application seeks to search Unit 1417, including the common areas of Unit 1417 and MINANG's bedroom, but specifically excluding Cho's bedroom.

6. Agents first went to the Target Location on September 19, 2017. At that time, FBI James Marinelli and I went to the Target Location in an effort to locate and interview Euncie Offre. Upon knocking on the door, a man who identified himself as Carlson Cho answered and told agents that Offre did not reside in the apartment, but instead was an acquaintance of Cho's roommate, whom Cho identified as MINANG. Cho also provided a phone number for MINANG, phone number (508) 203-0142. Agents used this phone number to contact MINANG and arrange the interview with him at a Panera Bread restaurant on September 22, 2017. When agents asked Cho about the vehicle MINANG drove, Cho described MINANG's vehicle as blue BMW.

7. On September 22, 2017, just prior to our interview of MINANG, agents located blue BMW in the parking lot of the Target Location bearing Massachusetts registration 1PD-337. According to records from Massachusetts Registry of Motor Vehicles, this vehicle is registered to a woman believed to be MINANG's mother. Agents saw this same vehicle parked in the Target Location's parking lot more recently on September 27, 2017.

8. On September 27, 2017, agents telephonically interviewed Cho, who indicated he was currently in the Dallas, Texas area visiting family. During my telephonic interview of Cho,

he stated that he had cashed a check for MINANG. Cho said that check was for $35,000. According to Cho, MINANG asked him to cash the check for him because he had lost his identification. Cho said he cashed the check and gave the $35,000 to MINANG. When asked, Cho said he did not know the source of the money.

9. As further described in my September 28, 2017 affidavit, after receiving the $275,250 into one of MINANG's accounts from a BEC fraud, a cashier's check was made payable to Cho, in the name of "C. Tah Cho."

10. On the morning of September 29, 2017, other agents from FBI and I arrested MINANG on the criminal complaint. At approximately 6:00 a.m., agents knocked on the front door to the Target Location. MINANG answered the door. Agents advised him that the FBI had a warrant for his arrest. MINANG indicated he understood and agents escorted him his bedroom to get additional clothing. MINANG walked to his bedroom which is located off the living room, to the left from the front entrance. The other bedroom, believed to be occupied by Cho, was to the right of the front entrance. At the time of the arrest, the only person inside the Target Location was MINANG.

11. Upon entering MINANG's bedroom and while he was getting fully dressed, I observed a laptop lying on top of his bed, a smartphone on the bed stand next to the bed, and a second smartphone on the windowsill.

Seizure of Computer Equipment and Data

12. As further described in Attachment B to the proposed warrant for the Target Location, this application seeks permission to seize records that might be found at the premises in whatever form they are found. In addition to seizing computer equipment (the laptop computer and smartphones in MINANG's bedroom), this application also seeks authorization to

search the content of any computers and smartphones in MINANG's bedroom and if necessary, copy the data on the computer by imaging the computers (including, if necessary, identifying any encryption data enabled on a computer, to copy such encryption data, including RAM memory collection, prior to imaging), as further described below. I submit that if a computer or electronic medium is found in MINANG's bedroom, there is probable cause to believe those records will be stored in that computer or electronic media, for at least the following reasons:

a. From my training, experience, and information provided to me by other agents, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related e-mail and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling business activities; keeping a calendar of business and other activities; arranging for business travel; storing pictures related to business activities; purchasing and selling inventory and supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of money online.

b. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online. I am also aware that the Consumer

Electronics Association estimated that in 2010, 86 percent of all U.S. households owned at least one computer.

c. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files generated at or to be used at a business, such as e-mail, word-processing documents, photographs, and spreadsheets.

d. From my training, experience, and information provided to me by other agents, I am aware that businesses and individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

e. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

13. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. In addition, based on my knowledge, training, and experience, I know that businesses and businesspeople often retain correspondence, financial, transactional, and other business records for years to identify past customers and vendors for potential future transactions; keep track of business deals; monitor payments, debts, and expenses; resolve business disputes stemming from past transactions; prepare tax returns and other tax documents; and engage in other business-related purposes.

14. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal

evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

15. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in

Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

Conclusion

16. Based on the foregoing, I submit there is probable cause to believe that the above described Target Location which is further described in Attachment A to the warrant application and warrant contains evidence, fruits, instrumentalities of violation of 18 U.S.C. § 1343 (wire fraud) and 18 U.S.C. § 1956(a)(1)(B) (money laundering).

Signed under the pains and penalties of perjury this 29th day of September, 2017.

Kevin M. McCusker
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 29th day of September, 2017.

THE HONORABLE M. PAGE KELLEY
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS